IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
Richmond Division

UNITED STATES OF AMERICA	)	
	)	
v.	)	Criminal Action No. 3:11CR13–HEH
	)	
PHILLIP A. HAMILTON,	)	
	)	
Defendant.	)	

MEMORANDUM OPINION
(Government's Motion to Admit into Evidence Electronic Messages Stored by the Defendant and Previously Exchanged Between the Defendant and His Spouse)

The defendant, Phillip A. Hamilton ("Hamilton"), is charged in a two-count Indictment with Federal Program Bribery and Extortion Under Color of Official Right. The case is set for trial with a jury beginning May 2, 2011. The matter is presently before the Court on the Government's Motion to Admit into Evidence Electronic Messages Stored by the Defendant and Previously Exchanged Between the Defendant and His Spouse. Both sides have filed memoranda of law supporting their respective positions. The Court heard oral argument and received evidence on April 6, 2011. For the reasons discussed below, the government's motion will be granted.

The electronic messages at issue were exchanged between Hamilton and his wife on August 16, 2006. Their relevance to the prosecution at hand does not appear to be in dispute. The messages were either transmitted or received on Hamilton's workplace computer. Hamilton opposes their admissibility on two grounds. First, he contends that the contents of his office computer were illegally seized by the FBI, in violation of his right of personal privacy. And, secondly, if lawfully seized, their disclosure would

trespass on the marital privilege.

In addition to serving as a member of the Virginia General Assembly, on August 16, 2006, Hamilton was employed by the Newport News Public Schools ("NNPS") in Newport News, Virginia. As a school employee, Hamilton had an assigned workplace computer and was afforded access to the NNPS electronic communications system. The relevant e-mails were sent and received by Hamilton using his NNPS work e-mail account. The government contends that these e-mails are essential to establish his state of mind, intent, and motive, and would be admissible under Federal Rule of Evidence 401.

Critical to the analysis of both questions before the Court is whether the NNPS had a computer workplace use policy in effect which limited Hamilton's expectation of privacy. The government concedes that the NNPS did not have a technology acceptable use policy in effect on August 16, 2006. NNPS, however, adopted a computer use and privacy policy on June 19, 2007. (Gov't's Mot. Admit Evidence, Ex. 4, ECF No. 17.) The policy was revised and republished on July 15, 2008. (Gov't's Mot. Admit Evidence, Ex. 5.) The revised policy provided in pertinent part:

> Privacy: Communications over the division's network shall be considered public information and handled as such. The NNPS Computer System authorized users must not have and shall have no expectation of privacy in their use of the Computer System. All information created, sent received, accessed, or stored in the NNPS Computer System is subject to inspection and monitoring at any time as authorized by the Superintendent or designee and may occur without notice to users.

(Gov't's Mot. Admit Evidence, Ex. 5, at 1.)

John J. Bowden, Jr. ("Bowden"), the supervisor of the NNPS computer network,

testified at the April 6, 2011 hearing that these policies were disseminated to all school personnel in 2007 and 2008. In addition, Bowden indicated that in 2008, a document entitled "Frequently Asked Questions," which reiterated the privacy policy, was electronically sent to all NNPS employees. (Gov't's Mot. Admit Evidence, Ex. 6.)

The evidence further revealed that forms acknowledging this policy were electronically signed in Hamilton's name on his assigned computer on February 1, 2008 and October 24, 2008. (Gov't's Mot. Admit Evidence, Ex. 5, at 7.) Bowden also testified that the NNPS computer system has a message or banner which appears on every computer screen at the time users log on, which clearly restates this policy. According to Bowden, in order to progress to the next step in the log-on process, the user must press a key to acknowledge this message, which process cannot be bypassed. The log-on banner contains the following message:

> This NNPS computer system including Internet and e-mail access is provided only for authorized use. All computers may be monitored to ensure that use is authorized and to verify operational security. All data stored or transmitted over this system may be monitored. Unauthorized use may subject the user to criminal prosecution and evidence of this use may be used for administrative or other adverse action.

(Gov't's Mot. Admit Evidence, Ex. 9, at 1.)

In opposition, Hamilton contends that the government's evidence falls short of demonstrating that he personally read the privacy policy or log-on banner or even electronically signed the acknowledgement. The evidence preponderates to the contrary.

Although no published workplace computer policy was in effect in August 2006, the above described policy had been conspicuously in effect for over two years when

federal agents executed a search warrant on September 2, 2009 and seized the contents of Hamilton's computer. The e-mails which the government seeks to introduce were discovered during an examination of messages stored on Hamilton's assigned computer.

As touched on above, Hamilton's opposition to the admissibility of the e-mails is based on a perceived violation of his Fourth Amendment right of privacy and the marital privilege. Neither affords him the protection he seeks under the facts of this case.

Turning first to his apparent Fourth Amendment argument, Hamilton maintains that in defining the boundaries of his expectation of privacy, the Court should focus on the day of the e-mail transmission, August 16, 2006, and not September 2, 2009, the day on which the stored contents of his computer were seized. Absent a published policy limiting workplace computer privacy in effect at the time the August 16, 2006 transmission was stored, Hamilton claims a reasonable expectation of privacy.[1]

It is now well settled that public employees have a reasonable expectation of privacy in their workplace. *O'Connor v. Ortega*, 480 U.S. 709, 717, 107 S. Ct. 1492, 1497 (1987). "Individuals do not lose Fourth Amendment rights merely because they work for the government instead of a private employer." *Id.* The Court in *O'Connor*, however, added a cautionary note. "Public employees' expectations of privacy in their offices, desks, and file cabinets, like similar expectations of employees in the private sector, may be reduced by virtue of actual office practices and procedures or by legitimate regulation." *Id.*

As the U.S. Court of Appeals for the Fourth Circuit noted in *United States v.*

[1] The validity of the search warrant is not presently at issue.

Simons, this workplace privacy limitation applies as well to computers and Internet communications.

> Simons did not have a legitimate expectation of privacy with regard to the record or fruits of his Internet use in light of [his employer's] Internet policy. . . . This policy placed employees on notice that they could not reasonably expect that their Internet activity would be private. Therefore, regardless of whether Simons subjectively believed that the files he transferred from the Internet were private, such a belief was not objectively reasonable after [his employer] notified him that it would be overseeing his Internet use.

206 F.3d 392, 398 (4th Cir. 2000); *see also Am. Postal Workers Union v. U.S. Postal Serv.*, 871 F.2d 556, 560 (6th Cir. 1989).

In *American Postal Workers Union*, the U.S. Court of Appeals for the Sixth Circuit concluded that employees had no reasonable expectation of privacy in their individual lockers in light of policies allowing locker inspections. Other reviewing courts seemed to have reached a similar conclusion. *See United States v. Angevine*, 281 F.3d 1130, 1133–35 (10th Cir. 2002); *Muick v. Glenayre Elecs.*, 280 F.3d 741, 743 (7th Cir. 2002). As Judge Posner commented in *Muick*, "the laptops were [Glenayre Electrics'] property and it could attach whatever conditions to their use it wanted to." *Id.*

In the immediate case, the NNPS policy made clear that the limitation on computer privacy applied not only to transmissions sent and received, but also to those that were *stored*. When the search warrant was executed on September 2, 2009, Hamilton was on long-standing notice that the contents of his computer were subject to inspection. He therefore lacked an objectively reasonable expectation of privacy in the

stored August 16, 2006 e-mails.[2]

The other facet of Hamilton's opposition is a claim of marital privilege. Few tenets of law are more fossilized than the privilege protecting confidential marital communication. Marital communications are presumptively confidential. *Blau v. United States*, 340 U.S. 332, 333, 71 S. Ct. 301, 302 (1951); *United States v. Parker*, 834 F.2d 408, 411 (4th Cir. 1987). If the nature and circumstances surrounding the communications, however, indicate that it was not intended to be confidential, then it is not privileged. *Wolfle v. United States*, 291 U.S. 7, 14, 54 S. Ct. 279, 280 (1934); *see also United States v. Madoch*, 149 F.3d 596, 602 (7th Cir. 1998).

Courts have uniformly held that the marital communications privilege can be waived. This commonly occurs "when the holder of the privilege . . . is in possession of the materials at issue and fails to take adequate precautions to maintain their confidentiality, i.e., negligent or inadvertent disclosures . . . ." *SEC v. Lavin*, 111 F.3d 921, 930 (D.C. Cir. 1997). The rationale underlying this implied waiver was explained by the U.S. Court of Appeals for the Ninth Circuit in *United States v. de la Jara*:

> When the disclosure [of privileged material] is involuntary, we will find the privilege preserved if the privilege holder has made efforts "reasonably designed" to protect and preserve the privilege. Conversely, we will deem the privilege to be waived if the privilege holder fails to pursue all reasonable means of preserving the confidentiality of the privileged matter.

973 F.2d 746, 750 (9th Cir. 1992) (citations omitted); *see also In re Horowitz*, 482 F.2d

---

[2] In his opposition, Hamilton relies in part on *Sprenger v. Rector and Board of Visitors of Virginia Tech*, No. 7:07CV502, 2008 WL 2465236 (W.D. Va. June 17, 2008). The facts in *Sprenger* are easily distinguishable in that neither Mr. nor Mrs. Springer had notice of the University's Electronic Communication Systems Policy.

72, 78 (2d Cir. 1973); *O'Leary v. Purcell Co., Inc.*, 108 F.R.D. 641, 644–46 (M.D.N.C. 1985).

Also instructive is *Banks v. Mario Indus. of Virginia, Inc.*, 274 Va. 438, 650 S.E.2d 687 (2007). In *Banks*, an employee of the defendant created a pre-resignation memorandum on a workplace computer. Defendant's employee handbook explicitly provided that there was no expectation of privacy regarding its computer network. The employee printed the document from the computer, conveyed it to his attorney seeking legal advice, and deleted the document from the system. The defendant's forensic computer expert retrieved the document from the computer's hard drive. The Supreme Court of Virginia found that the attorney-client privilege had been waived. "The privilege may be expressly waived by the client, or a waiver may be implied from the client's conduct." *Id.* at 454, 650 S.E.2d at 696 (citing *Commonwealth v. Edwards*, 235 Va. 499, 509, 370 S.E.2d 296, 301 (1988)); *see also Kansas v. Myers*, 640 P.2d 1245, 1249 (Kan. 1982).

In the present case, Hamilton was aware that his employer had access to the contents of his computer and took no steps to safeguard the electronic messages between him and his wife. At the very least, he could have deleted them from the system, which he did not. Therefore, the Court finds that the marital privilege was waived, and the government's motion will be granted.

An appropriate Order will accompany this Memorandum Opinion.

/s/
Henry E. Hudson
United States District Judge

Date: April 11, 2011
Richmond, VA